REMARKS

This application has been carefully reviewed in light of the Office Action dated June 30, 2008. Claims 1 to 13 are remain pending in the application, with Claims 14 to 16 having been canceled herein. Claims 1, 5 and 9 are the independent claims. Reconsideration and further examination are respectfully requested.

Claims 1 and 5 were objected to for an informality regarding allegedly incorrect grammar. The informality noted in the Office Action has been attended to by amendment. Reconsideration and withdrawal of the objection are respectfully requested.

Claims 1, 5 and 9 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly omitting essential steps. Without conceding the correctness of the rejections, the claims have nonetheless been clarified by amendment to include a case where the address is not within the range. Thus, reconsideration and withdrawal of the § 112 rejections are respectfully requested.

Claims 1, 5, 9 and 14 to 16 were rejected under § 103(a) over U.S. Publication No. 2002/0016858 (Sawada) and U.S. Patent No. 6,704,789 (Ala-Laurila), Claims 2, 3, 6, 7, 10 and 11 were rejected under § 103(a) over Sawada in view of Ala-Laurila and further in view of U.S. Patent No. 6,393,484 (Massarani), Claims 4, 8 and 12 were rejected under § 103(a) over Sawada in view of Ala-Laurila and further in view of U.S. Publication No. 2003/0041167 (French), and Claim 13 was rejected under § 103(a) over Sawada in view of Ala-Laurila and further in view of U.S. Publication No. 2002/0062485 (Okano). The rejections are respectfully traversed and the Examiner is requested to reconsider and withdraw the rejections in light of the following comments.

The present invention concerns determining whether or not to allow device to utilize a tentative network address in order to avoid address collision between devices. According to the invention, an address restriction apparatus (e.g., a router) determines address collision between devices by obtaining a tentative network address of a transmission source device that is generated by the transmission source device, and also obtains a local address unique to the transmission source device. The address restriction apparatus then determines whether the obtained tentative network address is a network address which is within an address range determined according to a predetermined rule and has been generated from the obtained local address unique to the transmission source device. If it is determined that the tentative address is not within the predetermined range, a message is sent to the transmission source device forbidding the use of the tentative network address. Likewise, if it is determined that the tentative network address is within the range, but has not been generated from the obtained local address unique to the transmission source device, the message forbidding the use of the address is sent to the transmission source device. On the other hand, if it is determined that the tentative network address is within the range and has been generated from the obtained local address, then the transmission source device is permitted to use the tentative address for communication on the network.

Referring specifically to the claims, amended independent Claim 1 is directed to an address restriction method executed by an address restriction apparatus on a network, comprising the steps of obtaining, from a message received from a transmission source device, a tentative network address generated by the transmission source device which is connected to the network, and a local address unique to the transmission source

device, determining whether the obtained tentative network address is a network address which is within an address range determined according to a predetermined rule and has been generated from the obtained local address unique to the transmission source device, in a case where the determining step determines that the tentative network address is the network address which is not within the address range determined according to the predetermined rule, sending a message to the transmission source device forbidding the use of the obtained tentative network address, in a case where the determining step determines that the tentative network address is the network address which is within the address range determined according to the predetermined rule and has been generated from the obtained local address unique to the transmission source device, permitting the transmission source device to use the tentative network address for performing communication on the network, and in a case where the determining step determines that the tentative network address is the network address which is within the address range determined according to the predetermined rule but has not been generated from the obtained local address unique to the transmission source device, sending a message to the transmission source device forbidding the use of the obtained tentative network address.

Claims 5 and 9 are computer medium and apparatus claims, respectively, that substantially correspond to Claim 1.

The applied art, alone or in any permissible combination, is not seen to disclose or to suggest the features of independent Claims 1, 5 and 9, and in particular, is not seen to disclose or to suggest at least the features of an address restriction apparatus i) determining whether an obtained tentative network address (which is obtained from a transmission source device) is a network address which is within an address range

determined according to a predetermined rule and has been generated from an obtained local address unique to the transmission source device, ii) in a case where it is determined that the tentative network address is the network address which is within the address range determined according to the predetermined rule and has been generated from the obtained local address unique to the transmission source device, permitting the transmission source to use the tentative network address for performing communication on the network, and ii) in a case where it is determined that the tentative network address is the network address which is within the address range determined according to the predetermined rule but has not been generated from the obtained local address unique to the transmission source device, or where it is determined that the tentative network address is not within the address range determined according to the predetermined rule, sending a message to the transmission source device forbidding the use of the obtained tentative network address.

The Office Action alleges that Sawada teaches the claimed obtaining and determining steps, as well as each of the "in a case" steps, but does not teach the feature of sending a message forbidding use of the tentative address. However, as Applicant understands Sawada, it merely determines the proper routing of messages by referring to a table and comparing a sub-net address, a MAC address, and a IP address in a table to determine if the message is authorized to be sent, and if not, the packet is discarded. Applicant fails to see where Sawada teaches the claimed determining step of "determining whether the obtained tentative network address is a network address which is within an address range determined according to a predetermined rule and has been generated from the obtained local address unique to the transmission source device." That is, the determination of the claimed invention is based on two parts: 1) whether the tentative

network address is within an address range based on a predetermined rule, and 2) whether the tentative network address is also generated from the obtained local address unique to the transmission source device. While the Office Action alleges that paragraphs [0255] and [0259] of Sawada teach these features, Applicant disagrees.

In this regard, Sawada teaches that a learned address table is employed to determine whether a user terminal is authorized to connect to a network. That is, subnet addresses and IP address are stored in correlation with one another in the table to determine if the terminal is authorized to connect to the network, and the learned table is searched for matching subnet addresses and IP addresses. However, Sawada is not seen to determine whether the address itself has been generated from an obtained local address unique to the transmission source device. Thus, Sawada is not seen to teach the claimed determining step of the invention.

Moreover, the Office Action admits that Sawada fails to teach the feature of sending a message to the transmission source forbidding the use of the tentative network address, but cites Ala-Lauria as allegedly making up for this deficiency of Sawada. Specifically, the Office Action alleges that column 1, line 66 to column 2, line 23 of Ala-Lauria teaches this feature. Applicant disagrees.

In this regard, it should first be noted that the claimed feature is more than merely sending a message forbidding use of a tentative network address. That is, in the invention, the sending of such message is initiated based on the claimed determination. That is, when the invention determines that the tentative network address is within a predetermined range determined according to a predetermined rule, but the address has not been generated from an obtained local address unique to the transmission source device,

then, in this case, the invention sends the message forbidding the use of the tentative network address. In contrast, the cited portion of Ala-Lauria merely teaches a convention DHCP request. According to the cited portion, when a computer wants to deallocate its IP address, which was assigned utilizing DHCP, it sends a DHCP release message to the server, whereby the user may not use the IP address any longer. However, if the user wants to continue using the address for a longer time, the user has to renew the use of the assigned IP address within a specified time. If the server accepts the renewal request, it sends an acknowledgment to the computer. If the server denies the renewal, it sends a DHCP non-acknowledgment which forces the user to immediately stop using the IP address and to initiate an entirely new IP address allocation process. Thus, while the server may inform the user that their request to continue using the same IP address has been denied, this denial is not tied to a determination that the tentative network address is within a predetermined range determined according to a predetermined rule, but the address has not been generated from an obtained local address unique to the transmission source device. Instead, the process is invoked in Ala-Lauria by the user, who already has permission to use the IP address, wanting to continue to use the address longer than a specified time. Therefore, Ala-Lauria is not seen to make up for the deficiencies of Sawada.

In view of the foregoing amendments and remarks, independent Claims 1, 5 and 9, as well as the claims dependent therefrom, are believed to be allowable.

No other matters having been raised, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

/Edward Kmett/

Edward A. Kmett
Attorney for Applicant
Registration No.: 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3800
Facsimile: (212) 218-2200

FCHS_WS 2502496v1